

#2

Docket No. 1614.1121/HJS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Nobuo YATSU et al.

Serial No.:

Filed: January 30, 2001

For: DATA CONVERTER

Group Art Unit:

Examiner:



**SUBMISSION OF CERTIFIED COPY OF PRIOR
FOREIGN APPLICATION IN ACCORDANCE WITH
THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s)
herewith a certified copy of the following foreign application(s):

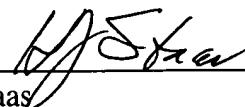
Japanese Patent Application No. 2000-57711
Filed: March 2, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing
date, as evidenced by the certified papers attached hereto, in accordance with the requirements
of 35 U.S.C. § 119.

Respectfully submitted,
STAAS & HALSEY LLP

Date: January 30, 2001

By: _____


H. J. Staas
Registration No. 22,010

700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

JCS64 U.S. PTO
09/771691
01/30/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

2000年 3月 2日

CERTIFIED COPY OF
PRIORITY DOCUMENT

出願番号
Application Number:

特願2000-057711

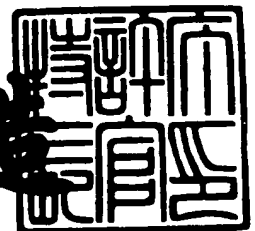
出願人
Applicant(s):

富士通高見澤コンポーネント株式会社

2000年12月 1日

特許庁長官
Commissioner,
Patent Office

及川耕造



【書類名】 特許願

【整理番号】 9960207

【提出日】 平成12年 3月 2日

【あて先】 特許庁長官 近藤 隆彦 殿

【国際特許分類】 G09C 1/00

【発明の名称】 データ変換装置

【請求項の数】 13

【発明者】

【住所又は居所】 東京都品川区東五反田 2 丁目 3 番 5 号 富士通高見澤コンポーネント株式会社内

【氏名】 谷津 信夫

【発明者】

【住所又は居所】 東京都品川区東五反田 2 丁目 3 番 5 号 富士通高見澤コンポーネント株式会社内

【氏名】 遠藤 孝夫

【特許出願人】

【識別番号】 595100679

【氏名又は名称】 富士通高見澤コンポーネント株式会社

【代理人】

【識別番号】 100070150

【住所又は居所】 東京都渋谷区恵比寿 4 丁目 2 0 番 3 号 恵比寿ガーデンプレイスタワー 3 2 階

【弁理士】

【氏名又は名称】 伊東 忠彦

【電話番号】 03-5424-2511

【手数料の表示】

【予納台帳番号】 002989

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9709404

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ変換装置

【特許請求の範囲】

【請求項 1】 データを変換する機能を備えたデータ変換装置であって、
時間を計時する計時手段と、

前記計時手段による計時時間に基づいて前記データ変換機能を使用不可な状態
にロックするロック手段と、

前記ロック手段によるロック状態を解除し、前記データ変換機能を再び使用可
能な状態に戻すロック解除手段とを備えたデータ変換装置。

【請求項 2】 前記ロック解除手段は、識別データを入力するための識別デ
ータ入力手段と、前記ロック状態を解除するために定めた識別基準データを記録
する識別基準データ記録部と、前記識別データ入力手段から入力された識別デー
タと前記識別基準データとを照合し、そのデータが一致したときに前記ロック状
態の解除を行う解除制御部とを含むことを特徴とする請求項 1 記載のデータ変換
装置。

【請求項 3】 前記識別データ入力手段は数字、文字、記号が入力可能な入
力キーであることを特徴とする請求項 2 記載のデータ変換装置。

【請求項 4】 前記識別データ入力手段は接触することにより座標位置によ
る入力可能な平面座標入力装置であることを特徴とする請求項 2 記載のデータ
変換装置。

【請求項 5】 前記識別データ入力手段は接触することにより座標位置によ
る入力可能な透明な平面座標入力部と、該平面座標入力部の背面側に設けられ
数字、文字、記号を表示する表示部とを有した入力表示装置であることを特徴と
する請求項 2 記載のデータ変換装置。

【請求項 6】 前記識別データ入力手段は使用者の指紋画像を入力する指紋
入力装置であることを特徴とする請求項 2 記載のデータ変換装置。

【請求項 7】 前記指紋入力装置は入力された指紋画面を細分して画素化し
、各画素の静電気量を測定して入力を行うことを特徴とする請求項 6 記載のデー
タ変換装置。

【請求項 8】 前記指紋入力装置は指紋入力面に押し当てられた指の指紋を光学的に撮影して入力を行うことを特徴とする請求項 6 記載のデータ変換装置。

【請求項 9】 前記ロック解除手段は、前記ロック状態を解除するために用いる識別基準データを記録する識別基準データ記録部と、前記データ変換装置を接続したコンピュータ側で入力され送信される識別データと前記識別基準データとを照合し、そのデータが一致したときに前記ロック状態の解除を行う解除制御部とを含むことを特徴とする請求項 1 記載のデータ変換装置。

【請求項 10】 前記識別基準データの入力及び前記識別データの入力は、前記コンピュータの入力装置を用いて行われることを特徴とする請求項 9 記載のデータ変換装置。

【請求項 11】 前記データ変換機能を使用不可とする時間を定めるための時間設定手段をさらに有することを特徴とする請求項 1 から 10 いずれか記載のデータ変換装置。

【請求項 12】 前記ロック手段が動作状態にあるか、否かを表示するロック状態表示手段をさらに有することを特徴とする請求項 1 から 11 いずれか記載のデータ変換装置。

【請求項 13】 請求項 1 から 12 いずれかに記載のデータ変換装置を用いたデータ漏洩防止機能付きのコンピュータ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は例えば小型コンピュータ等の携帯端末装置に適用されるデータ漏洩防止機能を備えたデータ変換装置に関し、より詳しくは計時手段を備え所定時間が経過した以降は所定の解除操作を行わないとデータの読出しができないようにした暗号カード、ICカード等のデータ変換装置に関する。

【0002】

【従来の技術】

近年、コンピュータネットワークや携帯電話等の情報・通信機器の普及は著しい。今後、社外に持ち出した携帯コンピュータ（携帯端末装置）から社内の情報

ネットワークにアクセスして情報を引出す等の用途がさらに増加するものと予想される。このような環境では使用者の不注意から携帯端末装置を紛失したり、或いは携帯端末装置が盗難に合って他人の手に渡る事態が発生する可能性がある。したがって、このような事態が生じた場合でも携帯端末装置内の重要データが他人により解読されないような手段を講じておくことが重要となっている。

【 0 0 0 3 】

そのために、従来から携帯端末装置内部のデータを変換して暗号化し、データのセキュリティを確保するために種々の暗号化ソフトや暗号化ハードウェアが検討され、提案されてきている。

【 0 0 0 4 】

例えば、携帯端末装置のセキュリティを確保する暗号化ハードウェアの1つとして暗号カードを用いた提案がある。この技術は所定の暗号カードを携帯端末装置にセットした場合だけその携帯端末装置が使用可能となるものである。よって、正規の使用者が暗号カードを保管しておくことで、暗号カードを持たない他人は携帯端末装置からデータの読出しができない。また一般にこの種の暗号カードには所定のパスワードやサイン或いは指紋を入力して照合する機能が付加されており、カード保持者が本来の使用者であるか、否かを識別することで安全性をより高めている。

【 0 0 0 5 】

【発明が解決しようとする課題】

しかしながら、使用者が上記暗号カードを携帯端末装置にセットし使用可能な状態で紛失する場合や、そのような状態で盗難に合う場合もある。このような場合、携帯端末装置は適性に使用可能状態となっており、他人に重要なデータを読取られることになり、未だセキュリティを十分に確保しているとは言い難い。

【 0 0 0 6 】

本発明は上述したような問題を解決するためになされたものであり、その主な目的は確実にデータの漏洩を防止できるコンピュータ用のデータ変換装置を提供することにある。

【 0 0 0 7 】

【課題を解決するための手段】

上記の目的は、請求項 1 に記載する如く、

データを変換する機能を備えたデータ変換装置であって、

時間を計時する計時手段と、

前記計時手段による計時時間に基づいて前記データ変換機能を使用不可な状態にロックするロック手段と、

前記ロック手段によるロック状態を解除し、前記データ変換機能を再び使用可能な状態に戻すロック解除手段とを備えたデータ変換装置により達成される。

【0008】

請求項 1 記載の発明によれば、データ変換装置は所定時間が経過するとデータ変換機能を使用不可のロック状態とする。よって、本データ変換装置を付属させた状態でコンピュータが他人の手に渡る事態となっても重要なデータが読み出されることを防止できる。

【0009】

上記計時手段はデータ変換装置に計時部を設ける場合だけではなく、接続されるコンピュータ側の計時部を利用することによっても実現できる。ここで計時すべき時間はコンピュータ側にデータ変換装置を接続したとき、コンピュータの使用を開始したとき等から所定時間としてもよし、時刻を特定してデータ変換機能を使用不可状態とするように設定してもよい。また、本発明でいうコンピュータは本来的には簡易に搬出可能な小型の携帯端末装置、例えばノート型、ハンドヘルド型、パームトップ型等の小型コンピュータであるが、例えば盗難に合ったときに運び出されてしまう可能性がある卓上用のコンピュータ等についても本発明のデータ変換装置を適用してもよい。

【0010】

上記ロック手段はデータ変換装置のデータ変換機能による処理を不可とする機構であれば特に限定されるものでなく、例えば所定時間を過ぎた時点でデータ変換装置内の配線をオフにする機構やデータ変換機能の処理に用いる鍵データを読み出し不可となるように設定すればよい。

【0011】

上記データ変換装置がロック状態になった後、正規の利用者によりロック状態を解除する手法としてデータ変換装置側だけでロック解除を行うという観点から、請求項 2 に記載する如く請求項 1 のデータ変換装置は、

前記ロック解除手段は、識別データを入力するための識別データ入力手段と、前記ロック状態を解除するために定めた識別基準データを記録する識別基準データ記録部と、前記識別データ入力手段から入力された識別データと前記識別基準データとを照合し、そのデータが一致したときに前記ロック状態の解除を行う解除制御部とを含む構成とすることができる。

【 0 0 1 2 】

請求項 2 記載の発明によれば、識別データ入力手段に入力された識別データと識別基準データ記録部内に保存されている識別基準データとが照合され、一致が確認されてからロック状態が解除される。よって、入力すべき識別データを知らない第 3 者にコンピュータが渡る場合があってもロック状態を解除されることはない。したがって、第 3 者によりコンピュータ内の重要データが読み出されることが防止できる。

【 0 0 1 3 】

そして、請求項 2 記載のデータ変換装置は請求項 3 に記載の如く、前記識別データ入力手段は数字、文字、記号が入力可能な入力キーである構成とすることができる。

【 0 0 1 4 】

また、請求項 2 記載のデータ変換装置は請求項 4 に記載の如く、前記識別データ入力手段は接触することにより座標位置による入力可能な平面座標入力装置である構成とすることができる。

【 0 0 1 5 】

また、請求項 2 記載のデータ変換装置は請求項 5 に記載の如く、前記識別データ入力手段は接触することにより座標位置による入力可能な透明な平面座標入力部と、該平面座標入力部の背面側に設けられ数字、文字、記号を表示する表示部とを有した入力表示装置である構成とすることができる。

【 0 0 1 6 】

また、請求項2記載のデータ変換装置は請求項6に記載の如く、前記識別データ入力手段は使用者の指紋画像を入力する指紋入力装置である構成とすることができる。

【0017】

上記請求項3から請求項6に記載の発明によれば、使用者が数字、文字、記号からなる入力キーを用いて入力するパスワードデータ、使用者が平面座標入力装置を用いて入力するサインデータ、使用者が入力表示装置の数字、文字、記号からなる入力キーを用いて入力するパスワードデータ或いは使用者が指紋入力装置を用いて入力する指紋データを識別データとして入力し、これらデータと対応するように予め設定され識別基準データ記録部に保管されている識別基準データとが照合され、一致が確認されるとロック状態が解除される。よって、第3者によりロック状態が解除されることはなく、コンピュータ内の重要データが読み出されることが確実に防止できる。

【0018】

また、請求項6記載のデータ変換装置は、請求項7に記載の如く前記指紋入力装置は入力された指紋画面を細分して画素化し各画素の静電気量を測定して入力を行う構成としてもよいし、請求項8に記載の如く前記指紋入力装置は指紋入力面に押し当てられた指の指紋を光学的に撮影して入力を行う構成としてもよい。

【0019】

さらに、前記データ変換装置がロック状態になった後、正規の使用者によりロック状態を解除する手法としてデータ変換装置とこのデータ変換装置が接続されるコンピュータとを協働させて解除を行うという観点から、請求項9に記載する如く請求項1のデータ変換装置は、

前記ロック解除手段は、前記ロック状態を解除するために用いる識別基準データを記録する識別基準データ記録部と、前記データ変換装置を接続したコンピュータ側で入力され送信される識別データと前記識別基準データとを照合し、そのデータが一致したときに前記ロック状態の解除を行う解除制御部とを含む構成とすることができる。

【0020】

請求項 9 記載の発明によれば、コンピュータ側で設定した識別データはデータ変換装置に送信され、識別基準データ記録部内に保存されている識別基準データと照合され、一致が確認されてからロック状態が解除される。よって、入力すべき識別データを知らない第 3 者にコンピュータが渡ってもロック状態を解除されるはことはない。したがって、第 3 者によりコンピュータ内の重要データが読み出されることが防止できる。

【 0 0 2 1 】

また、請求項 9 記載のデータ変換装置は請求項 1 0 に記載の如く、前記識別基準データの入力及び前記識別データの輸入は、前記コンピュータの入力装置を用いて行われる構成としてもよい。

【 0 0 2 2 】

請求項 1 0 記載の発明によれば、コンピュータ側に設けられた入力装置を用いて、ロック解除のための識別基準データ入力及び前記識別データ入力を行うことができる。よってデータ変換装置側の構成を簡素化できる。コンピュータ側の入力装置として入力キー、平面画像入力装置、指紋入力装置等を用いることができ、パスワード、サイン、指紋等を入力して識別データとすることができる。

【 0 0 2 3 】

さらに、請求項 1 から 1 0 いずれか記載のデータ変換装置は、請求項 1 1 に記載の如く、前記データ変換機能を使用不可とする時間を定めるための時間設定手段をさらに有する構成とすることができ、このような構成とすれば使用者の判断で適宜、データ変換機能を使用不可とする時間を変更することができる。例えば、コンピュータを使用する環境が紛失、盗難の虞がない場合にはロック状態に入る時間を長めに設定することでロック解除の作業を行うことなくコンピュータ操作を行うことができる。

【 0 0 2 4 】

上記時間設定手段として例えば上記入力キーを用いることができる。パスワードを識別データとするために入力キーを有するタイプのデータ変換装置である場合にはその入力キーを流用して時間設定を行うようにしてもよい。

【 0 0 2 5 】

またさらに、請求項 1 から 1 1 いずれか記載のデータ変換装置は、請求項 1 2 に記載の如く、前記ロック手段が作動状態にあるか、否かを表示するロック状態表示手段をさらに有する構成とすれば、データ変換装置のロック状態を速やかに判断できる。係る表示は、例えばデータ変換装置に表示部を設けてロック状態である旨の表示を行ってもよいし、小型の発光素子等を配設しこれを点灯することによりロック状態を知らせてもよい。

【 0 0 2 6 】

そして、請求項 1 3 に記載の如く、請求項 1 から 1 2 いずれかに記載のデータ変換装置を用いたデータ漏洩防止機能付きのコンピュータとして構成することもできる。このようなコンピュータは第 3 者により内部の重要データが読み出されることが防止できる。

【 0 0 2 7 】

【発明の実施の形態】

以下、本発明のデータ変換装置を暗号カードとして実現した実施例を図面に基づいて説明する。

【 0 0 2 8 】

図 1 は本発明の第 1 実施例に係る暗号カード 1 の外観を示す斜視図である。本第 1 実施例の暗号カード 1 ではロック状態を解除するための識別データとして指紋を用いる。

【 0 0 2 9 】

図 1 において、暗号カード 1 は指紋入力装置 1 0、ロック状態を表示する表示部 1 3 並びにロック状態に入るまでの時間の設定及びその変更を行うため等に用いる入力キー 1 2 を有している。指紋入力装置 1 0 は指紋を登録するとき及びロック解除のために指紋の入力を行うときに使用者の指を当てる入力画面 1 1 を有している。指紋入力装置 1 0 は入力画面 1 1 の下部には指紋認識のための指紋検出部、検出した指紋に基づいて識別データとしての指紋データを生成するデータ生成部等を備えている。ここで指紋を検出する手法としては周知の画像認識技術を用いることができ、例えば入力画面 1 1 を細かい画素に分割しその各画素の静電気量を測定する方法や入力画面 1 1 に光を当て指紋を光学的な手法で読取る方法

等を用いて指紋入力装置 1 0 を構成することができる。

【 0 0 3 0 】

さらに、暗号カード 1 は多数ピンを備えたコネクタ部 1 4 を端部に有し、例えば図 2 に示すコンピュータ 1 0 0 のスロット 1 1 0 に対し矢印 X 方向に挿入して接続できるようになっている。

【 0 0 3 1 】

図 3 は暗号カード 1 の構成とこれを接続するコンピュータ 1 0 0 の一部構成を示したブロック図である。暗号カード 1 は制御部 1 5、計時部 1 6、暗号化・復号部 1 7、記憶装置部 1 8 及び前述した指紋入力装置部 1 0、入力キー部 1 2、表示部 1 3 を有している。これらの各部は情報連絡（バス）1 9 を介して接続され、CPU 等からなる制御部 1 5 によりロック解除制御と共に暗号カードの全体的な制御がなされるようになっている。

【 0 0 3 2 】

また、暗号カード 1 はコンピュータ 1 0 0 との接続のためのインターフェース 2 0 を備えている。構成の一部が示されたコンピュータ 1 0 0 は、前述したスロット部 1 1 0 の他、制御部 1 2 0、データファイルを保管する記憶装置 1 3 0、入力キー 1 4 0 及び暗号カード 1 との接続のためのインターフェース 1 5 0 等を備えている。上記暗号カード 1 側のインターフェース 2 0 及びコンピュータ 1 0 0 側のインターフェース 1 5 0 を介して、コンピュータ 1 0 0 側から暗号カード 1 側へのコマンド信号、暗号カード 1 側からコンピュータ 1 0 0 側へのステータス信号及びこの両者の間でのデータの送受信がなされるようになっている。なお、上記インターフェース 2 0 及びインターフェース 1 5 0 は、例えば IC カードの標準的な規格である PCMCIA (Personal Computer Memory Card International Association) に準拠して構成されている。

【 0 0 3 3 】

本暗号カード 1 はコンピュータ 1 0 0 側で作成されたデータを暗号化処理し、データの漏洩を防止するデータ変換機能を本来的に備えている。すなわち、暗号カード 1 をコンピュータ 1 0 0 に接続すると、コンピュータ 1 0 0 側で作成されたデータは暗号カード 1 側で暗号化処理され、コンピュータ 1 0 0 側に戻されて

記憶装置部 1 3 0 に保管される。また、この暗号化データを読出すときにはコンピュータ 1 0 0 側から暗号カード 1 側へ暗号処理済データを送信して復号処理を受けることでデータが利用可能となるような設定である。この暗号カード 1 側におけるデータの暗号化と復号化のデータ処理は制御部 1 5 の下で暗号化・復号手段 1 7 が実行する。よって、暗号カード 1 をコンピュータ 1 0 0 に接続しなければデータの読出しを行うことができず、使用者が暗号カード 1 を厳しく管理していれば、例えコンピュータ 1 0 0 だけが第 3 者に渡るような事態となってもデータが漏洩することはない。なお、ここで用いることができる暗号化手法は、コンピュータ業界で標準的に使用されている DES、トリプル DES、FEAL 或いはインターネットで一般的に用いられている RSA、楕円曲線暗号等である。

【 0 0 3 4 】

しかしながら、暗号カード 1 がコンピュータ 1 0 0 に接続された状態で、紛失或いは盗難に遭う場合もあり得る。そこで、本暗号カード 1 はデータ漏洩をより確実に防止できるように、さらにロック手段を備えているものである。

【 0 0 3 5 】

このロック手段は計時手段に基づいて設定される所定時間が経過した後は、前述した暗号化及び復号処理を行う暗号化・復号部 1 7 を使用不可の状態にロックするものである。このようなロック手段を備えていれば、例え暗号カード 1 がコンピュータ 1 0 0 に接続された状態で第 3 者に渡る事態が生じても設定時間が経過した後は暗号カード 1 がロック状態となるのでそれ以降のデータ読出しが不可能となりデータの漏洩を抑制することができる。

【 0 0 3 6 】

上記時間の設定は、例えばコンピュータ 1 0 0 に暗号カード 1 を接続してからの所定時間或いはコンピュータ 1 0 0 により実際の作業を開始してからの所定時間とするように自動的に設定するようしてもよいし、使用者が適宜の時間を入力できるような手段を付加してもよい。本暗号カード 1 では図 3 に示すように、計時部 1 6 と共に時間設定を行える入力キー 1 2 を備えており、設定時間を適宜変更できるようになっている。制御部 1 5 は使用者が入力キー 1 2 を介して定めた設定時間と計時部 1 6 からの時間情報を読み込んで比較を行い、計時した時間が

設定時間を超えたと判断したときには暗号カード 1 を使用不可の状態にロックするように制御する。

【 0 0 3 7 】

本実施例の暗号カード 1 のように時間設定の変更を可能とする入力キー 1 2 を設ければ、使用者がコンピュータ 1 0 0 を扱う環境、すなわちデータ漏洩のリスク度に応じて設定時間を変更することが可能となる。特に安全な環境下でコンピュータ 1 0 0 を使用する場合にはロック状態とする必要がなく、またロック状態となった後には後述するロック解除の操作が必要となるので上記入力キー 1 2 のような時間設定手段を設けるとことでよりユーザフレンドリーな暗証カードとすることができる。なお、暗号カード 1 は表示部 1 3 を有しており、設定時間が経過してロック状態に入った時には、例えば「LOCK」と表示し、使用可能な状態であるときには「OK」を表示して、コンピュータ 1 0 0 のデータが読出し可能な状態か、否かが確認できるようになっている。

【 0 0 3 8 】

そして、上記暗号カード 1 は、ロック状態に入った後に、使用者がこれを解除できるようにロック解除手段を備えている。使用者は自己の指紋を識別基準データとして記憶装置 1 8 内に予め保管しておき、ロック状態を解除するとき入力画面 1 1 から指紋データを再入力して照合を行い前記ロック状態の解除を行うようにしている。すなわち、上記指紋の識別基準データはコンピュータ 1 0 0 の初期設定において指紋入力装置 1 0 の入力画面 1 1 から使用者の指紋を入力し、これを識別基準データとして記憶装置部 1 8 に登録する。ロック解除を行うときには使用者は登録に用いた指を入力画面 1 1 に当て指紋を入力すると、制御部 1 5 が記憶装置部 1 8 から読み出した識別基準データと入力されたデータを照合する。制御部 1 5 により、一致が確認されるとロック状態を解除される。

【 0 0 3 9 】

なお、本暗号カード 1 の記憶装置部 1 8 は識別基準データ記録部として機能すると共に、上記暗号化・復号部 1 7 がデータの暗号化・復号処理において用いる鍵データも保管しており、制御部 1 5 によりロック状態が設定されるとこの鍵データが読み出せなくなり、暗号化・復号処理が実行できなくなるようになっている。

【 0 0 4 0 】

図 4 には上記暗号カード 1 の制御部 1 5 が実行する基本的なルーチンを示すフローチャート 2 0 0 を示している。図 4 のルーチンはコンピュータ 1 0 0 側に暗号カード 1 が適性に接続されることにより実行される。

【 0 0 4 1 】

ステップ 2 0 1 ではコンピュータ 1 0 0 側の記憶装置 1 3 0 に保管されているデータを暗号カード 1 側で復号処理してから読み出す操作、及びコンピュータ 1 0 0 側で作成したデータを暗号カード 1 側で暗号化処理してから再びコンピュータ 1 0 0 側の記憶装置 1 3 0 に保管する操作が行える処理可能状態である。ステップ 2 0 2 では制御部 1 5 が計時部 1 6 から計時している時間を読み込み、ステップ 2 0 3 へ進む。

【 0 0 4 2 】

ステップ 2 0 3 では制御部 1 5 がステップ 2 0 2 で読み込んだ計時部 1 6 からの計時時間が設定時間を超えたか、否かを判断する。計時時間が設定時間を超えていなければ上記ステップ 2 0 1 に戻って上記各ステップを繰返す。一方、計時時間が設定時間を超えていれば、ステップ 2 0 4 で指紋データ入力可能な状態に入り、続くステップ 2 0 5 で制御部 1 5 は入力された指紋データと基準指紋データとの照合を行い一致するか、否かが判断する。同一のデータであると判断した時にはステップ 2 0 1 に戻り操作可能な状態が維持される。

【 0 0 4 3 】

一方、制御部 1 5 はステップ 2 0 4 で指紋データの入力が無かった場合やステップ 2 0 5 で入力された指紋データと基準指紋データとが一致しないと判断した場合には、ステップ 2 0 6 へ進み、暗号カードが使用できないロック状態とする。なお、このときには前述したように表示部 1 3 に「LOCK」が表示されることになる。

【 0 0 4 4 】

さらに、次ぎのステップ 2 0 7 でコンピュータ 1 0 0 側との接続が維持されているか、否かが判断される。接続が維持されていると判断されると上記ステップ 2 0 4 に戻り同様の処理が繰返される。なお、ステップ 2 0 4、2 0 5、2 0 6

、207の処理が繰返される状態は前述したロック状態に相当する。ステップ207でコンピュータ100側との接続が断たれたと判断すると、ステップ208へ進み、制御部15により実行されていた上記ルーチンを終了する。

【0045】

本実施例では識別データとして使用者の指紋を用いるので他人に盗用される虞が少なく、識別データの厳密な照合がなされる。よって、暗号カード1がコンピュータ100に接続された状態で第3者に渡る事態が生じても設定時間が経過した後は暗号カード1がロック状態となるのでそれ以降のデータ読出しが不可能となりデータの漏洩を確実に防止できる。

【0046】

図5は本発明の第2実施例に係る暗号カード2の外観を示す斜視図である。本第2実施例の暗号カード2はロック状態を解除するための識別データとして入力キー22から入力されるパスワードを用いる。なお、暗号カード2は第1実施の暗号カード1と基本構成は同様であるので、異なる点について説明を加え重複する点は省略する。

【0047】

本第2実施例の暗号カード2は、入力キー22、表示部23、コネクタ部24等を有している。暗号カード2では、ロック解除時に用いるための識別基準データとして、初期設定で入力キー22からパスワードを暗号カード2内の記憶装置内に記録させる。ロック状態を解除させようとする時には同じパスワードを入力することでロックを解除することができる。

【0048】

前記第1実施例で指紋を用いたのに対し、本実施例では識別データとしてパスワードを用いる点が異なっている。本実施例では、計時時間の設定や変更を行う際に用いる入力キー22を流用する簡易な構成でデータ漏洩防止機能を備えた暗号カードを提供することができる。

【0049】

図6は本発明の第3実施例に係る暗号カード3の外観を示す斜視図である。本第3実施例の暗号カード3はロック状態を解除するための識別データとして入力

表示装置 3 2 から入力される使用者のサインを用いる。なお、暗号カード 3 についても第 1 実施の暗号カード 1 と基本構成は同様であるので、異なる点について説明を加え重複する点は省略する。

【 0 0 5 0 】

本第 3 実施例の暗号カード 3 は、入力表示装置 3 2、コネクタ部 3 4 等を有している。入力表示装置 3 2 は、接触することにより座標位置による入力が可能である透明な平面座標入力部 3 2 A と、この平面座標入力部の背面側に設けられ数字、文字等を表示可能な表示部 3 2 B とで構成されている。

【 0 0 5 1 】

暗号カード 3 では、ロック解除時に用いるための識別基準データとして、初期設定で平面座標入力部 3 2 A からサインを暗号カード 3 内の記憶装置内に記録させる。ロック状態を解除させようとする時には同じサインを入力することでロックを解除することができる。

【 0 0 5 2 】

前記第 1 実施例で指紋を用いたのに対し、本実施例では識別データとしてサインを用いる点が異なっている。本実施例では使用者の筆跡の癖を反映したサインを識別データに用いるので他人に盗用される虞が少なく、確実な照合が可能である。

【 0 0 5 3 】

なお、本第 3 実施例では平面座標入力部 3 2 A と共にロック状態等の表示が可能な表示部 3 2 B を有する入力表示装置 3 2 を用いている。そこで、本第 3 実施例の変形例として識別データの入力要求時に表示部 3 2 B 上に数字、文字等を表示させるように変更を加え、この数字等から入力する識別データとしてパスワードを採用することも可能である。さらに他の変形例として表示部 3 2 B を省略し、単にサインの入力を行う平面座標入力部 3 2 A で構成した入力装置としたてもよい。

【 0 0 5 4 】

さらに図 7 から図 9 に基づいて本発明の第 4 実施例について説明する。
前述した実施例は暗号カードでは、暗号化・復号の処理を不可とするロック処理

とこれを解除するロック解除処理を暗号カード側で行っていたが、第4実施例では暗号カード4とこれが接続されるコンピュータ300との協働で行う。

【0055】

図7は暗号カード4の外観を示す斜視図である。本実施例の暗号カード4は外部に入力装置、表示装置を有しておらずコネクタ部44のみを有した簡易な構成となっている。本実施例では前述した実施例で行っていた識別基準データの登録、ロック解除のために識別データの inputs はコンピュータ300側で行う。

【0056】

図8は暗号カード4の構成とこれを接続するコンピュータ300の一部構成を示したブロック図である。暗号カード4は制御部45、計時部46、暗号化・復号部47、記憶装置部48を有している。これらの各部はバス49を介して接続され、制御部45によりロック解除制御と共に暗号カードの全体的な制御がなされる。

【0057】

また、暗号カード4はコンピュータ300との接続のためのインターフェース41を備えている。構成の一部が示されたコンピュータ300は図2に示したコンピュータ100と同様な外観を有し、制御部320、データファイルを保管するハードディスク等からなる記憶装置330、入力キー340、表示部360及び暗号カード4との接続のためのインターフェース350等を備えている。上記暗号カード4側のインターフェース41及びコンピュータ300側のインターフェース350を介して、コンピュータ300側から暗号カード4側へのコマンド信号、暗号カード4側からコンピュータ300側へのステータス信号及びこの両者の間でのデータの送受信がなされるようになっている。

【0058】

本暗号カード4においてもコンピュータ300側で作成されたデータを暗号化処理して漏洩を防止する機能を本来的に備えており、暗号カード4側の制御部45、計時部46、暗号化・復号部47、記憶装置部48が果たす機能は前述した第1実施例の制御部15、計時部16、暗号化・復号部17、記憶装置部18と同様である。

【 0 0 5 9 】

ただし、識別データの入力はコンピュータ 3 0 0 側で行い、その入力データを暗号カード 4 側に送信して用いるようにしている点が前述した実施例とは異なっている。コンピュータ 3 0 0 側に設けた入力装置で取扱うことができるデータ、例えば入力キーを用いたパスワードデータ、指紋入力装置による指紋データ、音声入力装置による音声データ、画像入力装置により入力された顔画像データ等、多くのデータを識別データとして用いることができるが、本実施例ではコンピュータ 3 0 0 に備えられている入力キー 3 4 0 を用いて入力できるパスワードを識別データとする場合について説明する。

【 0 0 6 0 】

上記暗号カード 4 についても予め定めた設定時間が経過した後は、前述した暗号化及び復号処理を行う暗号化・復号部 4 7 を使用不可の状態にロックされるようになっている。本実施例では制御部 4 5 は使用者が定めた第 1 の設定時間と計時部 4 6 からの時間情報を読み込んで比較を行い計時時間が第 1 の設定時間を超えていた場合にはロック準備に入り、さらに第 2 の設定時間と計時部 4 6 からの時間情報を読み込んで比較を行い、これについても計時時間が第 2 の設定時間を超えていた場合には暗号カード 4 を使用不可とする状態にロックする構成となっている。この点については後のフローチャートで説明する。

【 0 0 6 1 】

なお、本実施例の暗号カード 4 の場合、時間の設定、変更はコンピュータ 3 0 0 の入力キー 3 4 0 を用いて行い、またロック状態に入った時はコンピュータ 3 0 0 の表示部 3 6 0 に「LOCK」と表示して、コンピュータ 3 0 0 のデータが読出し可能な状態か、否かが確認できるようしてもよい。

【 0 0 6 2 】

そして、上記暗号カード 4 は前記第 1 実施例から第 3 実施例の暗号カードとは異なるロック解除機構を備えている。識別データであるパスワードの入力はコンピュータ 3 0 0 側の入力キー 3 4 0 を用いて行い、照合に用いる基準パスワードの保管とロック解除時に入力されるパスワードの照合は暗号カード 4 側で行うようになっている。すなわち、本実施例の場合、上記パスワードの識別基準データは

コンピュータ 1 0 0 の初期設定において入力キー 3 4 0 から使用者がパスワードを入力し、これを暗号カード 4 側に送信して識別基準データとして記憶装置部 4 8 に予め登録する。ロック解除を行うときにも使用者は登録に用いたパスワードをコンピュータ 1 0 0 側の入力キー 3 4 0 から入力するとこれを暗号カード 4 側に送信し、制御部 4 5 が記憶装置部 4 8 から読み出した識別基準データと入力されたデータを照合する。制御部 4 5 により一致が確認されるとロック状態が解除されるようになっている。

【 0 0 6 3 】

図 9 には上記暗号カード 4 の制御部 4 5 とコンピュータ 3 0 0 が協働して実行する基本的なルーチンを示すフローチャート 4 0 0 を示している。図 9 中で点線で示したステップは暗号カード 4 側で行われている処理を示している。図 9 のルーチンはコンピュータ 3 0 0 側に暗号カード 4 が適性に接続されることにより実行される。

【 0 0 6 4 】

ステップ 4 0 1 で暗号化・復号処理のコマンド信号がコンピュータ 3 0 0 側から暗号カード 4 側へ入力され、続いてステップ 4 0 2 でコンピュータ 3 0 0 側の記憶装置 3 3 0 に保管されているデータを暗号カード 4 側で復号処理してから読み出す操作、及びコンピュータ 3 0 0 側で作成したデータを暗号カード 4 側で暗号化処理してから再びコンピュータ 3 0 0 側の記憶装置 3 3 0 に保管する操作が行える処理可能状態となる。

【 0 0 6 5 】

次に、ステップ 4 0 3 では暗号カード 4 側の制御部 4 5 が計時部 4 6 で計時している時間を読み込み、ステップ 4 0 4 で計時時間が第 1 の設定時間を越えたか、否かを判断する。この第 1 の設定時間は前述した本来的に設定された時間に相当し、この第 1 の設定時間を計時部 4 6 による計時時間が越えるとロック準備状態に入る。

【 0 0 6 6 】

上記ステップ 4 0 4 で計時時間が第 1 の設定時間を超えていなければ上記ステップ 4 0 1 に戻って上記各ステップを繰返す。一方、計時時間が第 1 の設定時間

を超えていれば、ステップ405で暗号カード4側からコンピュータ300側へステータス信号を送る。

【0067】

ステップ406で暗号カード4内の制御部45が計時部46で計時している時間を読み込み、ステップ407で計時時間が第2の設定時間を越えたか、否かを判断する。ここでの第2の設定時間はパスワードの入力待ち状態の時間である。ステップ407で制御部45が読込んだ計時時間が第2の設定時間を越えたと判断すると、直ちにステップ411へ進み、暗号カード4を使用不可とするロック状態に入る。制御部45が読込んだ計時時間が第2の設定時間を越えていなくときにはステップ408でパスワードデータ入力可能な状態に入る。続くステップ409で、コンピュータ300側の入力キー340から入力されたパスワードデータがコマンド信号として暗号カード4側に送信される。

【0068】

ステップ410で暗号カード4の制御部45は入力されたパスワードデータと基準パスワードデータとの照合を行い一致するか、否かが判断する。同一のデータであると判断した時にはステップ401に戻り操作可能な状態が維持される。

【0069】

一方、ステップ410で入力されたパスワードデータと基準パスワードデータとが一致しないと判断された場合には、ステップ411へ進み暗号カード4が使用できないロック状態とする。

【0070】

さらに、次ぎのステップ412で暗号カード4とコンピュータ300側との接続が維持されているか、否かが判断される。接続が維持されていると判断されると上記ステップ405に戻り同様の処理が繰返される。ステップ412でコンピュータ300側との接続が断たれたと判断すると、ステップ413へ進み、制御部45及びコンピュータ300により実行されていた上記ルーチンを終了する。

【0071】

本実施例では識別データとしてパスワードを用い、その入力はコンピュータ300側の入力装置を流用して簡素化し、識別データの登録・監視は暗号カード4

で行うようになっている。よって、従来のコンピュータの回路構成に変更を加えることなく暗号カード4側を簡易な構成で製造することができる。

【0072】

なお、上記実施例の暗号カードではPCMCIAに準拠したインターフェースを用いたがこれに限らず、USB等の他のインターフェースを採用することも勿論可能である。また、上記実施例では暗号カードを示しデータ変換機能として暗号化・復号機能を使用不可の状態にロックする例を示したが、これに限らず実質的にカードの機能を停止させるものであれば他の機能を使用不可とするによしてもよい。

【0073】

また、データ変換機能を使用不可とする時間の設定は特定の時刻、例えば10時になったら使用不可とする、というような設定を行うようにしてもよい。

【0074】

以上、本発明の好ましい実施例について詳述したが、本発明は係る特定の実施形態に限定されるものではなく、特許請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。

【0075】

【発明の効果】

以上詳述したところから明らかなように、

請求項1記載の発明によれば、データ変換装置は所定時間が経過するとデータ変換機能を使用不可のロック状態とする。よって、本データ変換装置を付属させた状態でコンピュータが他人の手に渡る事態となっても重要なデータが読み出されることを防止できる。

【0076】

また、請求項2記載の発明によれば、識別データ入力手段に入力された識別データと識別基準データ記録部内に保存されている識別基準データとが照合され、一致が確認されてからロック状態が解除される。よって、入力すべき識別データを知らない第3者にコンピュータが渡る場合があってもロック状態を解除されることはなく、コンピュータ内の重要データが読み出されることが確実に防止で

きる。

【 0 0 7 7 】

また、請求項 3 から請求項 8 に記載の発明によれば、使用者が数字、文字、記号からなる入力キーを用いて入力するパスワードデータ等を識別データとして入力し、これらデータと対応するように予め設定され識別基準データ記録部に保管されている識別基準データと照合され、一致が確認されるとロック状態が解除される。よって、第 3 者によりロック状態が解除されるはことはなく、コンピュータ内の重要データが読み出されることが確実に防止できる。

【 0 0 7 8 】

また、請求項 9 に記載の発明によれば、コンピュータ側で設定した識別データはデータ変換装置に送信され、識別基準データ記録部内に保存されている識別基準データと照合され、一致が確認されてからロック状態が解除される。よって、入力すべき識別データを知らない第 3 者にコンピュータが渡ったてもロック状態を解除されるはことはない。

【 0 0 7 9 】

また、請求項 1 0 に記載の発明によれば、コンピュータ側に設けられた入力装置を用いて、ロック解除のための識別基準データ入力及び前記識別データ入力を行うことができる。よってデータ変換装置側の構成を簡素化できる。

【 0 0 8 0 】

また、請求項 1 1 に記載の発明によれば、使用者の判断で適宜、データ変換機能を使用不可とする時間を変更することができ、コンピュータを使用する環境が紛失、盗難の虞がない場合にはロック状態に入る時間を長めに設定することでロック解除の作業を行うことなくコンピュータ操作を行うことができる。

【 0 0 8 1 】

また、請求項 1 2 に記載の発明によれば、データ変換装置のロック状態を速やかに判断できる。

【 0 0 8 2 】

そして、請求項 1 3 に記載の発明によれば、第 3 者により内部の重要データが読み出されることが防止できるデータ漏洩防止機能付きのコンピュータとして提供

することができる。

【図面の簡単な説明】

【図 1】

図 1 は本発明の第 1 実施例に係る暗号カードの外観を示す斜視図である。

【図 2】

図 2 は、図 1 に示した暗号カードを接続するコンピュータの外観を示す斜視図である。

【図 3】

図 3 は、図 1 に示した暗号カードの構成と図 2 に示したコンピュータの一部構成を示したブロック図である。

【図 4】

図 4 は図 1 に示した暗号カードの制御部が実行する基本的なルーチンを示すフローチャートである。

【図 5】

図 5 は本発明の第 2 実施例に係る暗号カードの外観を示す斜視図である。

【図 6】

図 6 は本発明の第 3 実施例に係る暗号カードの外観を示す斜視図である。

【図 7】

図 7 は本発明の第 4 実施例に係る暗号カードの外観を示す斜視図である。

【図 8】

図 8 は、図 7 に示した暗号カードの構成とこれが接続されるコンピュータの一部構成を示したブロック図である。

【図 9】

図 9 は、図 8 に示した暗号カードの制御部とコンピュータが実行する基本的なルーチンを示すフローチャートである。

【符号の説明】

- | | |
|---------|-------------------|
| 1、2、3、4 | 暗号カード（データ変換装置） |
| 10 | 指紋入力装置（識別データ入力手段） |
| 12 | キー入力部（時間設定手段） |

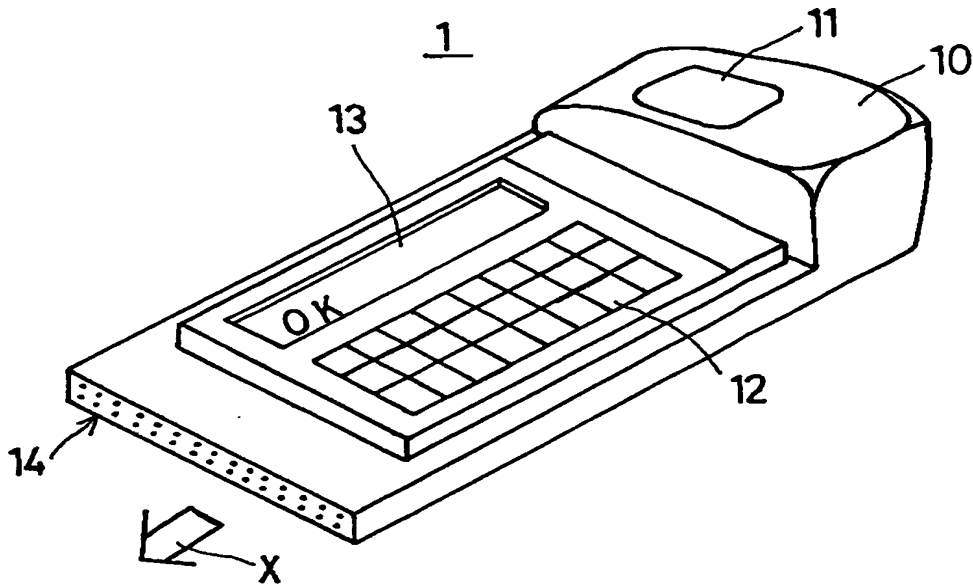
1 3	表示部（ロック状態表示手段）
1 5	制御部（解除制御部）
1 6	計時部
1 7	暗号化・復号部
1 8	記憶装置（識別基準データ記録部）
1 0 0	コンピュータ

【書類名】

図面

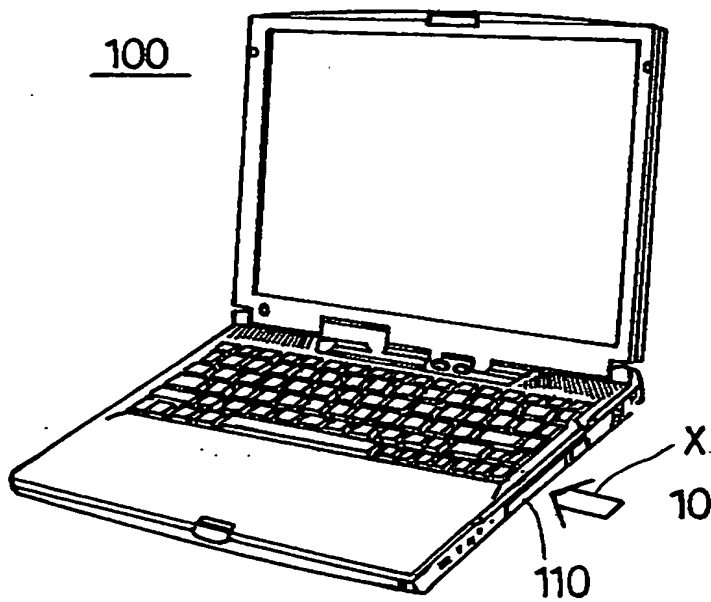
【図 1】

本発明の第1実施例に係る暗号カードの外観を示す斜視図



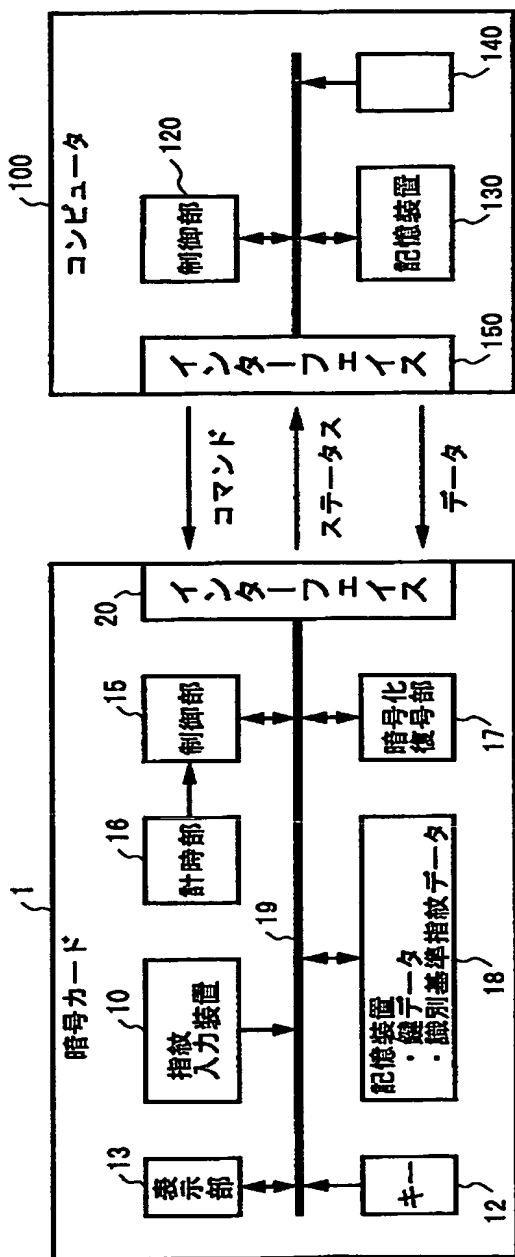
【図 2】

図 1 に示した暗号カードを接続するコンピュータの外観を示す斜視図



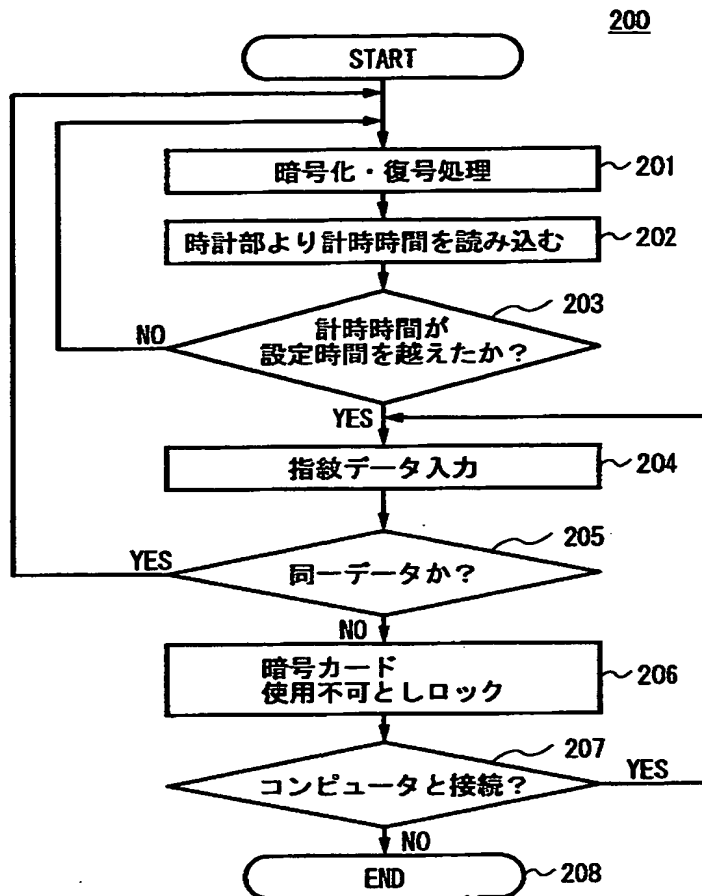
【図 3】

図1に示した暗号カードの構成と図2に示したコンピュータの一部構成を示したブロック図



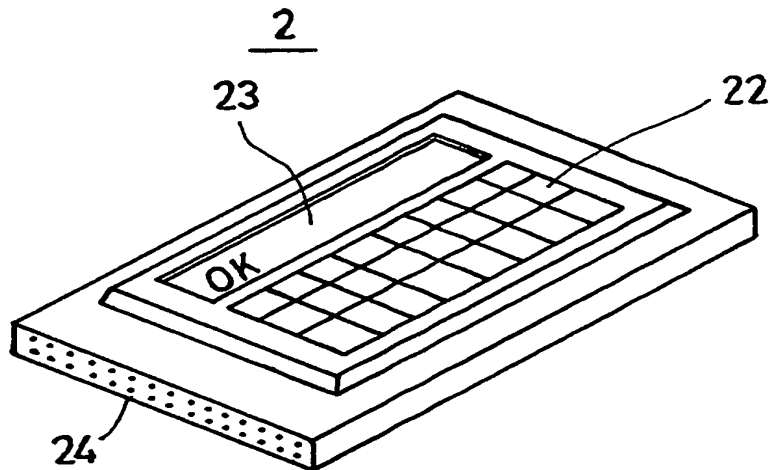
【図 4】

図1に示した暗号カードの制御部が実行する基本的なルーチンを示すフローチャート



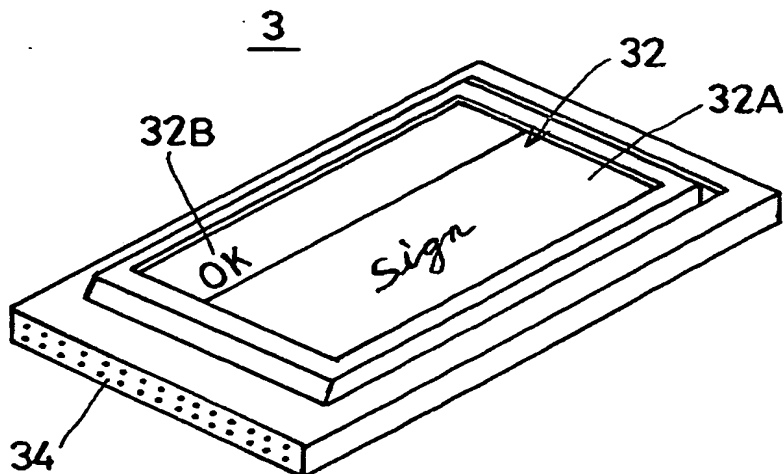
【図5】

本発明の第2実施例に係る暗号カードの外観を示す斜視図



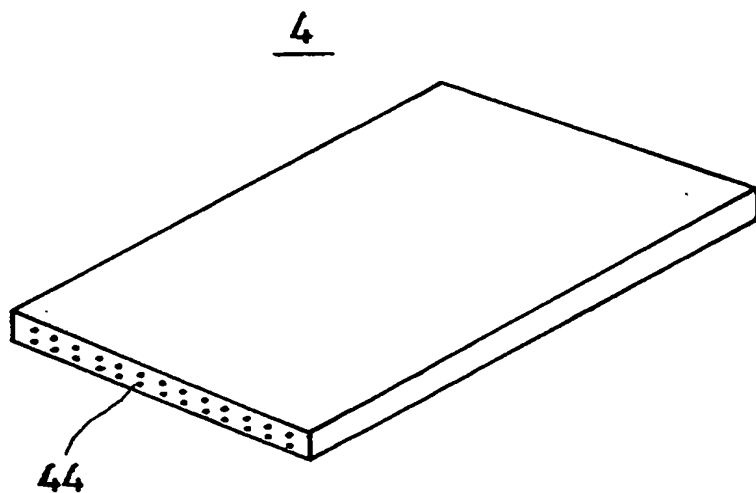
【図6】

本発明の第3実施例に係る暗号カードの外観を示す斜視図



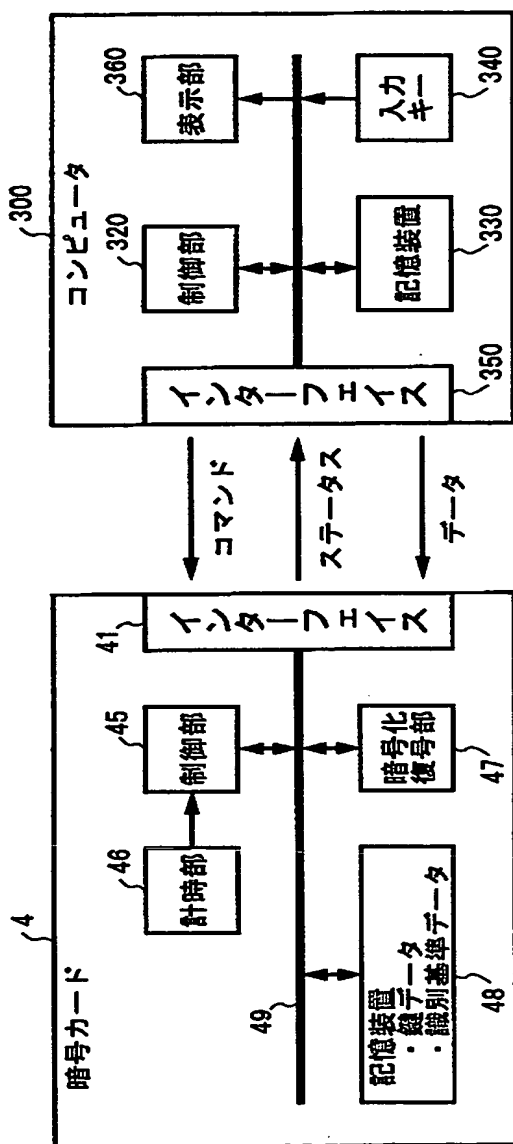
【図7】

本発明の第4実施例に係る暗号カードの外観を示す斜視図



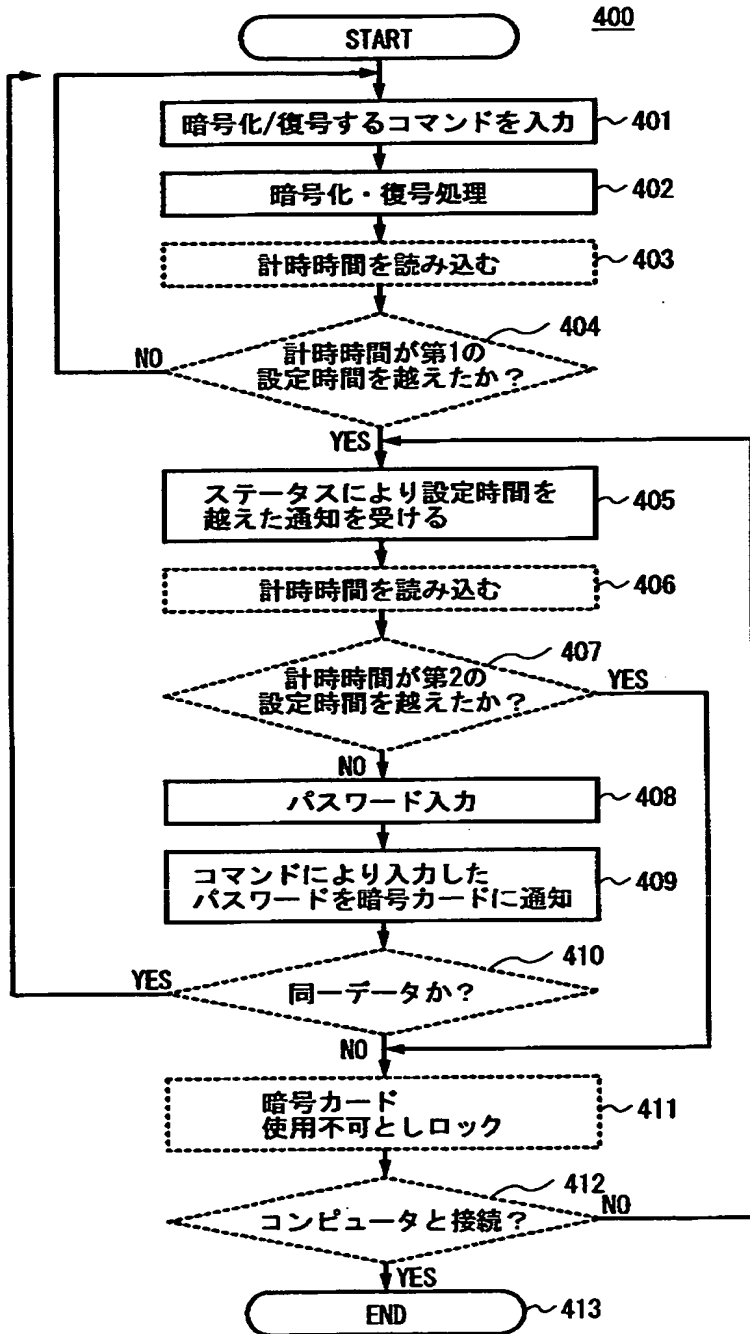
【図 8】

図7に示した暗号カードの構成とこれが接続されるコンピュータの一部構成を示したブロック図



【図 9】

図8に示した暗号カードの制御部とコンピュータが
実行する基本的なルーチンを示すフローチャート



【書類名】 要約書

【要約】

【課題】 確実にデータの漏洩を防止できるコンピュータ用のデータ変換装置を提供する。

【解決手段】 データを変換する機能を備えたデータ変換装置であって、時間を計時する計時手段と、前記計時手段による計時時間に基づいて前記データ変換機能を使用不可な状態にロックするロック手段と、前記ロック手段によるロック状態を解除し、前記データ変換機能を再び使用可能な状態に戻すロック解除手段とを備えたデータ変換装置である。

【選択図】 図3

出 願 人 履 歴 情 報

識別番号 [595100679]

1. 変更年月日	1995年 7月13日
[変更理由]	新規登録
住 所	東京都品川区東五反田2丁目3番5号
氏 名	富士通高見澤コンポーネント株式会社